



DEPARTMENT OF THE NAVY

DIRECTOR, SPACE AND NAVAL WARFARE
INFORMATION TECHNOLOGY CENTER
2251 LAKESHORE DRIVE
NEW ORLEANS, LA 70145-0001

SPAWARINFOTECHCENINST 5520.1
ITC201

04 Jun 2001

SPAWARINFOTECHCEN INSTRUCTION 5520.1

Subj: PERSONNEL SECURITY PROGRAM

Ref: (a) SECNAVINST 5510.30A
(b) SPAWARINFOTECHCENINST 5530.1
(c) DOD 5200.2-R
(d) DODD 5200.28

1. Purpose. To provide procedures for the administration of Space and Naval Warfare Information Technology Center (SPAWARINFOTECHCEN) Personnel Security Program in support of references (a) through (d).

2. Cancellation. NAVRESINFOSYSOFFINST 5520.1 and ITCNOTE 5530 of 16 May 00

3. Policy. All employees at SPAWARINFOTECHCEN will be required to have at least a favorable National Agency Check or National Agency Check with a written Inquiry (NAC/NACI) completed and on file in the Security Office.

4. Background

a. Reference (a) establishes the basic policy of the Department of the Navy (DON) security program. No person shall be appointed or retained as a civilian employee in the DON; accepted or retained in the Navy; granted a personnel security clearance; assigned to sensitive duties or granted access to classified information; unless appointment, acceptance, retention, clearance, or assignment is clearly consistent with the interests of national security.

b. Reference (a) has established that duties performed by employees not requiring a security clearance have as a minimum a NAC or NACI investigation completed to determine their trustworthiness.

5. Procedures

a. A NACI is required to support suitability determination for federal employees assigned to Non-Sensitive or Noncritical-Sensitive duties without access to classified information.

(1) The command Personnel Security Officer will be the contact point for processing government employees for the NACI.

(2) The government employee will be required to complete a Standard Form (SF) 86 (Questionnaire for National Security Positions), the SF 87 (Fingerprint Card), a resume or equivalent, and an OF 306 (Declaration of Federal Employment).

(3) The packet will be submitted to Office of Personnel Management for processing. The results will be returned to the command Security Office and retained.

(4) The contractor employee will work with his/her company security office to complete the necessary packet for submission by them for a NAC Investigation. A copy of the packet and the date of submission will be sent to the command Personnel Security Officer to be retained. When the investigation is sent to the Defense Security Service, a copy of the record of receipt will be provided to the command Personnel Security Officer. When the results of the security determination are received by the contracting company, a copy should be sent to the Personnel Security Officer, SPAWARINFOTECHCEN (ITC201).

b. An Access National Agency Check with written Inquiries (ANACI) is required for Federal employees in Noncritical-Sensitive positions who will require access to Confidential and Secret classified information. The ANACI request uses the same forms and procedures as the NACI request, but indicates "ANACI-09B" under item A "Type of Investigation."

c. Personnel security clearances will be granted on a "need to know" basis per information contained in reference (a). For ease of accountability, personnel security will publish a security access list containing all military and civilian personnel with their current security access. If it is none it will state none. This list will be retained by all departments, divisions and branches to ensure only authorized personnel have required access to classified information.

d. Access by non-U.S. citizens to government automated information systems will be authorized only by the Secretary of the Navy, as stated in reference (d).

5. Position Classification

a. All employee positions will be designated as Critical-Sensitive, Noncritical-Sensitive, or Nonsensitive per reference (c).

b. The responsibility for determining the position designation will fall to the Physical Security Review Committee as stated in reference (b), whose members will include all Directorate Directors or their designees.

6. Continuous Evaluation of Eligibility

a. Information reflecting on an individual's loyalty, reliability, and trustworthiness from a security perspective will be reported to the Command Security Manager. All command elements, particularly personnel, security, legal, medical, and supervisory personnel must understand that information which could place an individual's loyalty, reliability, and trustworthiness in question has to be evaluated from a security perspective. Personnel must be alert to behavior indicating unexplained affluence, financial instability, alcohol and drug abuse, mental or emotional instability, or criminal conduct that is potentially significant to an individual's security status.

b. Supervisors should act to identify problem areas at an early stage and to direct personnel to programs designed to counsel and assist them when they are experiencing financial, medical, or emotional difficulties.

c. Co-workers have an equal obligation to advise their supervisor or appropriate security officials when they become aware of information with potentially serious security significance regarding someone with access to classified information or employed in a sensitive position.

d. When derogatory or questionable information is acquired about an individual who holds a security clearance or assignment to sensitive civilian duties, the appropriate determination authority must reevaluate the individual's eligibility for access or assignment. The command Security Manager will make a recommendation to the Director, upon initial receipt of credible derogatory information, whether to suspend access to classified information and/or continue assignment to a sensitive position, pending final decision by the appropriate determination authority. The Director will determine, whether, on the basis of all the facts available upon receipt of the initial derogatory information, if it is in the interest of national security to take interim action to suspend or limit an individual's access to classified information or reassign the individual to other nonsensitive duties until a final determination is made. The Department of the Navy, Central Adjudication Facility (DONCAF) will suspend access for civilian employees, if not already accomplished by the command, when a letter of intent to revoke a security clearance is issued.

e. Supervisors will comment on eligibility of persons for continued access to classified information and discharge of security responsibilities in conjunction with regularly scheduled performance appraisals of military and civilian personnel whose duties entail access to classified information.

f. A security clearance, which was administratively withdrawn or lowered, may be reinstated to the previous level of eligibility if access requirements for official duties so warrant.

7. Action

a. Personnel Security Officer:

(1) Reports to the Security Manager.

(2) Ensures that all military and civilian personnel who are to handle classified information or be assigned to sensitive duties are appropriately cleared and that requests for personnel security investigations are properly prepared, submitted, and maintained. Ensures Department of Defense military and civilian personnel complete and sign an SF 312, Classified Information Nondisclosure Agreement, before being given initial access to classified material.

(3) Ensures that individual's personnel security investigation, clearance, and access are recorded.

(4) Publishes a security access list on a quarterly basis or more frequently as circumstances dictate.

(5) Ensures all background investigations are updated as needed or required.

(6) Ensures all position categories receive the investigation needed for implementation.

b. Directorates will:

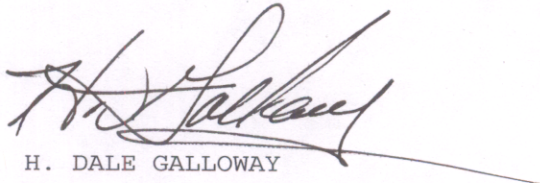
(1) Indicate on the Facility Access Card Request (SPAWARINFOTECHCEN 5512/1), the position classification required for the individual.

(2) Review the security access list on a quarterly basis to determine changes and report the changes to the Personnel Security Officer.

8. Forms. The following forms mentioned in this directive are stocked in the Security Office (ITC201).

- a. SF 86, Questionnaire for National Security Positions.
- b. SF 87, Finger Print Card.
- c. SF 312, Classified Information Non-disclosure Agreement.
- d. OF 306, Declaration of Federal Employment.
- e. OPNAV 5510/413, Personnel Security Action Request.
- f. SPAWARINFOTECHCEN 5512/1 (4-01), Facility Access Card Request.

9. Report. The Quarterly Security Access Review contained in paragraph 7b(2) above, has been assigned report control symbol SPAWARINFOTECHCEN 5520-1.



H. DALE GALLOWAY

Distribution: SPAWARINFOTECHCENINST 5218.1
Lists A, B, C, D, E, and F

CORs will ensure contractors receive and comply with this instruction.

Managers will ensure all SPAWARINFOTECHCEN personnel receive and comply with this instruction.